REMARKS

Claims 1-34 are pending, with claims 1, 12, 23 and 33 being independent. Claims 9-11, 20-22 and 30-34 have been cancelled without prejudice. Claims 1, 3, 12 and 14 have been amended. New claims 35-42 have been added. No new matter has been added. Reconsideration and allowance of the above-referenced application are respectfully requested.

Rejections Under 35 U.S.C. §§ 102 & 103

Claims 1-6, 8-9, 12-20, 23-29, and 33 stand rejected under 35 U.SC. 102(e) as allegedly being anticipated by Raley et al. (United States Publication Number 2003/0196121). Claims 7 and 18 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Raley et al. in view Leah et al. (United States Patent Number 6,986,039). Claims 10-11 and 21-22 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Raley et al. in view of Pensak et al. (United States Patent Number 6,449,721). Claims 30-31 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Raley et al. in view over Larose (United States Publication Number 2002/0087876). Claim 32 and 34 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Raley et al. in view over Larose and in further view of Non-Patent Literature "PageRecall: The Key to Document Protection, Authentica, Inc., Whitepaper. http://www.authentica.com/products/white" (hereinafter "PageRecall"). These contentions are respectfully traversed.

Independent claim 23 recites, "a client that sends a request to a server when an action is to be taken with respect to an electronic document local to the client; the server that receives the

request, and in response to the client, the server obtains and sends a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure; and wherein the client uses the authentication program to identify a current user and control the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document." (Emphasis added.) Raley et al. fail to disclose this subject matter.

Raley et al. describe a "system and method for securely distributing content by automatically deploying security components. The system includes a server having content stored thereon, a client device having a standard application program for accomplishing a task related to the content, and a rights management module operatively coupled to the server and said client device and configured, upon a request to access the content, to determine if security components are coupled to the application program. The rights management module downloads and installs the security components on the client device if the security components are not coupled to the application program." See Raley et al. at Abstract.

However, Raley et al. make very clear that the security components are delivered to the client before the client is given access to the content. See e.g., Raley et al. at ¶s [0057] & [0064]. Thus, Raley et al. does not describe sending the security components to the client in response to a request received from the client to an action "with respect to an electronic document local to the client", as claimed. It is noted that the Office Action omits the claim language, "local to the client", when explaining the rejection of claim 23. See 09-20-2007 Office Action at page 2.

Thus, the Office has failed to address all the elements of claim 23, and independent claim 23 should be in condition for allowance for at least the above reasons.

Independent claim 1 has been amended to include the language of cancelled claim 9. Claim 1 now recites:

> receiving, at a server, a request from a client to take an action with respect to an electronic document; retrieving a document identifier from the request; determining whether user authentication is needed based on the document identifier and the action; sending information specifying an acceptable authentication procedure; receiving an authentication procedure update request from the client; obtaining, at the server and in response to the request, a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure; and sending the authentication program to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document.

(Emphasis added.) As described, for example, in the present application:

> Additionally, the request 350 can represent multiple communications between the client 310 and the server 320. The client 310 can first communicate to the server 320 that the action has been requested, and the client requests to know whether authentication is to be performed, and if so, how authentication is to be performed. The information identifying the server 320 and the document 305 can be included in the document itself, and the server 320 can determine whether user authentication is needed based on the information identifying the document 305 and the nature of the requested action. The server 320 can respond as to whether authentication is needed, and if so, the type of authentication to be used, including

> potentially multiple types of acceptable authentication mechanisms, from which the client 310 can choose which one to use. If the client 310 does not already have the specified authentication functionality, the client 310 can then request a corresponding authentication update.

See Specification at ¶ [0055].

Nothing in Raley et al. teaches or suggests the subject matter of claim 9 (now amended claim 1). In the rejection of claim 9, the Office cites to ¶ [0066] of Raley et al., which states:

> FIG. 6 illustrates another example of a method of operation of the preferred embodiment. In step 602, security module 237 is directed to retrieve a document 222 from distributor server 220 server. In this example, document 222 is "clear content," i.e., is not encrypted or otherwise obscured or limited and does not have any use restrictions. Document 222 is returned by server 220 to security module 237 in step 604. Because document 222 is not signed, or encrypted, or otherwise marked as content that needs to be handled by security module 237, security module 237 recognizes that it is no longer required. In step 606, security module 237 notifies browser 232 that browser 232 should request document 222 directly by sending the original request for content to server 220. Security module 237 then removes itself as a running component, i.e., inactivates, in step 608 to preserve resources of client computer 230. In step 610, browser 232 then resubmits the request for document 222 that was originally sent by the security module 237. Distributor server 220 then delivers documents 222 directly to browser 232 in step 612.

See Raley et al. at ¶ [0066]. Nothing in this portion of Raley et al. or any other portion of Raley et al. suggests retrieving a document identifier from the request, determining whether user authentication is needed based on the document identifier and the action, sending information specifying an acceptable authentication procedure, and receiving an authentication procedure

update request from the client, as recited in amended claim 1. Thus, claim 1 should be in condition for allowance for at least this reason.

Claim 3 has been amended to be in independent form. Newly independent claim 3 recites:

> receiving, at a server, a request from a client to take an action with respect to an electronic document; obtaining, at the server and in response to the request, a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure; sending the authentication program to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document; receiving an updated authentication procedure; receiving a subsequent request from the client to take the action with respect to the electronic document; obtaining, in response to the subsequent request, a new software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the updated authentication procedure; and sending the new software program to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document.

(Emphasis added.) As described, for example, in the present application:

> Thus, the client 310 can be transparently updated with a new authentication process as a result of sending the request 350 to the server 320. The specific mechanism(s) of authentication is therefore configurable, and end-to-end delivery of authentication components can be performed without the user being aware of the update. If an administrator changes the authentication procedure to be used for a document, all clients that attempt to perform an action that requires the

> specified authentication with respect to that document can be automatically and transparently updated to be able to authenticate using the newly specified mechanism. An authentication procedure can even be changed between sequential actions on a document, and thus a new request 350 can result in a new authentication process 315 being delivered for the same action to be performed on an already delivered document.

See Specification at ¶ [0059].

Nothing in Raley et al. teaches or suggests the subject matter of claim 3. In the rejection of claim 3, the Office cites to ¶ [0092] and item 1410 of FIG. 14 in Raley et al. But this portion of Raley et al. merely states:

> In step 1402 security module 237 of client computer 230 loads an instance of a rendering application, browser 232 in the preferred embodiment. Browser 232 requests to load a third party add in program, such as DLL, in step 1404. Security module 237 intercepts the request and querys local database 225 including a list of trusted certified third party add in programs in step 1406. If security module 237 does not find the third party program that is attempting to load, security module 237 contacts a trusted server to update its database of trusted third party programs that are certified in step 1408. If the third party program is found in the updated list, security module 237 permits the loading of the third party program into the rendering engine in step 1410. If the determination in step 1406 is that the program is certified by being listed in database 225, the method goes directly to step 1410. If the determination in step 1408 is that the program is not in the updated database as being certified, loading is prohibited in step 1412.

See Raley et al. at ¶ [0092]. This portion of Raley et al. relates to loading of other code, not an updated authentication program. Nothing in this portion of Raley et al. or any other portion of Raley et al. suggests receiving a subsequent request from the client to take the action with

respect to the electronic document, obtaining, in response to the subsequent request, a new software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the updated authentication procedure; and sending the new software program to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document, as recited in amended claim 3. Thus, claim 3 should be in condition for allowance for at least this reason.

Claim 14 has also been rewritten in independent form and contains features similar to claim 3. Newly independent claim 14 recites:

> receiving a request from a client to take an action with respect to an electronic document; obtaining, in response to the request, an authentication process; sending the authentication process to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document; receiving a subsequent request from the client to take the action with respect to the electronic document; obtaining, in response to the subsequent request, a new authentication process; and sending the new authentication process to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document.

(Emphasis added.) Thus, for reasons similar to claim3, claim 14 should be in condition for allowance.

Independent claim 12 has been amended to include the language of cancelled claim 20. Claim 12 now recites:

> receiving a request from a client to take an action with respect to an electronic document; retrieving a document identifier from the request; determining whether user authentication is needed based on the document identifier and the action; sending information specifying an acceptable authentication procedure; receiving an authentication procedure update request from the client; obtaining, in response to the request, an authentication process; and sending the authentication process to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document.

(Emphasis added.) Thus, for reasons similar to claim 1, claim 12 should be in condition for allowance.

New claims 35-42 recite features similar to examined claims 2-9. Neither Leah et al., Pensak et al., Larose, nor PageRecall cure the noted deficiencies of Raley et al. Thus, each of dependent claims 2, 4-8, 13, 15-19, 24-29 and 35-42 should be allowable based on their respective base claims and the additional recitations they contain. For example, new claims 36 and 42 should also be allowable for reasons similar to those addressed above with respect to claims 3 and 1. In addition, the rejections of claims 9-11, 20-22 and 30-34 have been obviated by the cancellation of these claims without prejudice. Thus, all of the now pending claims should be in condition for allowance, and a formal notice of allowance is respectfully requested.

Conclusion

The foregoing comments made with respect to the positions taken by the Examiner are not to be construed as acquiescence with other positions of the Examiner that have not been explicitly contested. Accordingly, the above arguments for patentability of a claim should not be construed as implying that there are not other valid reasons for patentability of that claim or other claims.

Please apply any excess claims fees, and any other necessary charges or credits, to deposit account 06-1050.

Respectfully submitted,

Date: Dec. 20, 2007

William E. Hunter
Reg. No. 47,671

Fish & Richardson P.C.
PTO Customer No. **021876**
Telephone: (858) 678-5070
Facsimile: (858) 678-5099